

Mac OS X Consoliero

Einstieg und Gebrauch des Terminals für Power User.

Mac OS X Consoliero – Teil 2:
Troubleshooting und System Maintenance.

Christoph Müller, PTS

Mac OS X Consoliero – Teil 2: Troubleshooting und System Maintenance.

Inhaltsverzeichnis

Alle Warennamen werden ohne Gewährleistung der freien Verwendbarkeit benutzt und sind möglicherweise eingetragene Warenzeichen. Jegliche Bewertungen basieren auf den Erfahrungen des Autors und sind nicht signifikant.
Das Copyright liegt beim Autor. Die Serie „Mac OS X Consoliero" ist jedoch Shareware und darf für nichtkommerzielle private Zwecke frei verwendet werden. Diese Bestimmung schliesst Ausbildung und kommerzielle Verteilung zwingend aus. Bei Fragen zur Verwendung kontaktieren Sie den Autor bitte unter: chm@pts.ch.

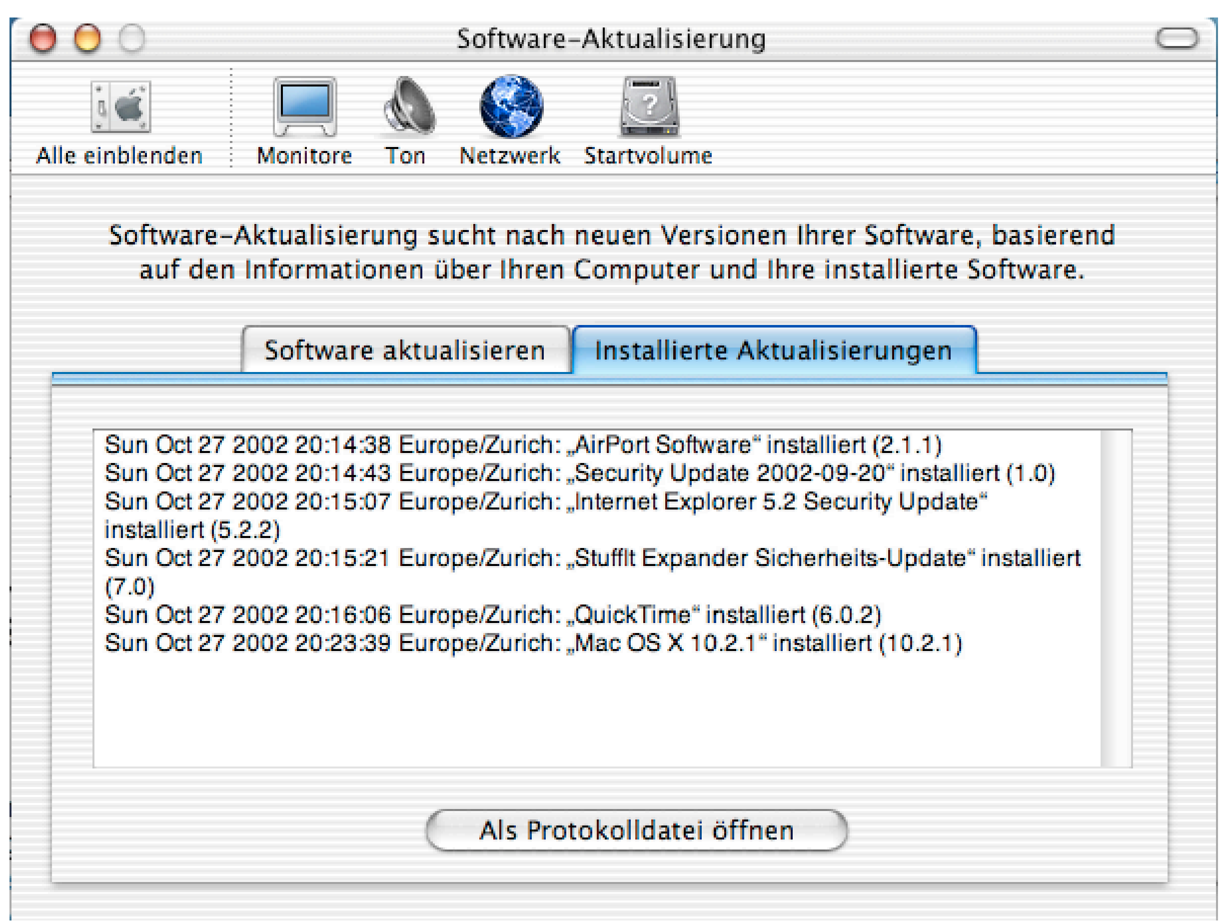
Mac OS X Consoliero – Teil 2:
Troubleshooting und System Maintenance.

Einleitung

Warum geht es nicht weiter mit Terminal Befehlen? Sollte es eigentlich! Jedoch sind einige Fragen an mich herangtragen worden, welche sich vor allem auf die Unsicherheit in Bezug auf das neue OS X beziehen. Deshalb habe ich mich entschieden, im zweiten Teil auf allgemeine Support Aspekte und erst im nächsten Teil auf weitere Terminal Befehle, welche wir für den Support auch brauchen, einzugehen.

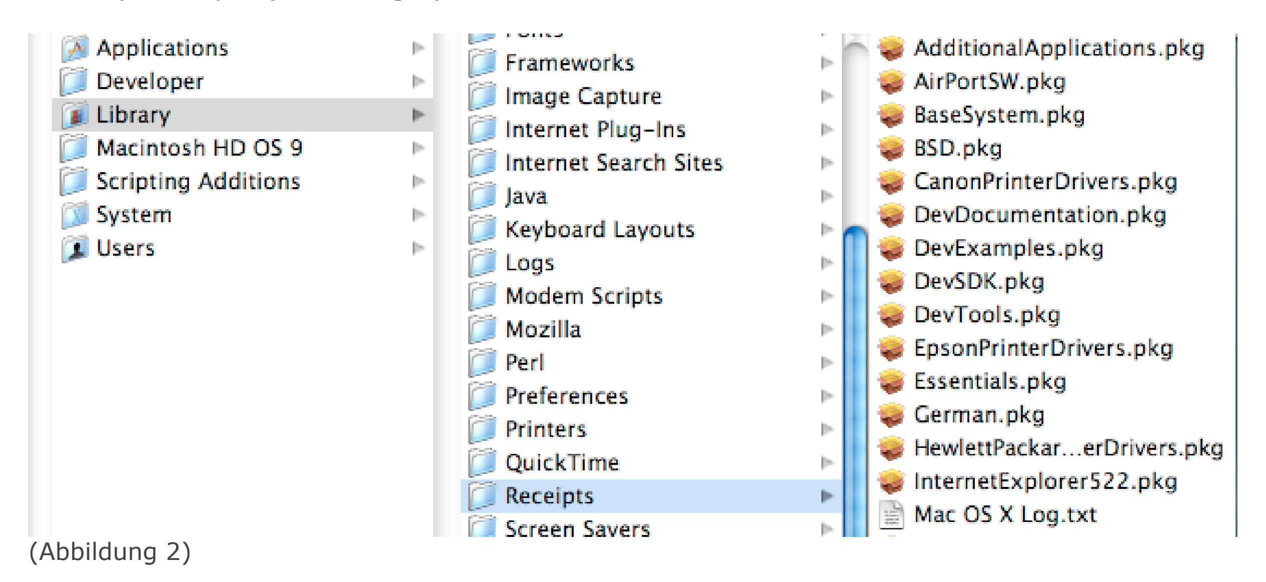
Software installieren und deinstallieren

Ein wichtiger Teil des Systemunterhaltes ist die installierten Komponenten von OS X auf dem Laufenden zu halten. Mit seinem BSD Kern braucht OS X zweifellos mehr updates als das OS 9. Mit sicherheitskritischen Updates von Systemkomponenten wie SSH werden regelmässig Lecks gestopft. Mac OS X automatisiert diesen Vorgang mit dem Programm „Software Aktualisierung", welches sich über die Systemeinstellungen öffnen lässt. Dort lässt sich auch die Liste der eingespielten Updates einsehen, (Abbildung 1).



(Abbildung 1)

Manchmal kommt es vor, dass im Logfile der Update (Abbildung 1) ein Fehler angezeigt wird. Oder dass ein ausgeführtes Update nicht in der Liste erscheint. Um hier einzugreifen macht es Sinn, das Update nochmals auszuführen. Um OS X im Glauben zu lassen er habe ein Update noch nicht gemacht um es erneut auszuführen muss man das zum Upgrade gehörende „receipt file" löschen. Diese Files befinden sich unter: /Library/Receipts (Abbildung 2).



(Abbildung 2)

Die „receipts files" sind nach dem Update Package Namen benannt. Das Löschen des entsprechenden Files macht, das OS X davon ausgeht dass das Update nie installiert worden ist.
Dieses Vorgehen funktioniert auch wenn Sie ein inoffizielles Update eingespielt haben und nun das offizielle von Apple einspielen wollen.

Kontrollieren Sie ebenfalls bei einer Systemaktualisierung, welche „receipts file" noch liegen geblieben sind. Vor allem solche welche ein System weiter aktualisert haben, als die Version welche Sie mit der System CD eingespielt haben. Starten Sie dann von Hand den System Aktualiesierer unter den Systemeinstellungen. Eine weiter Anomalie einer Aktualisierung ist, dass alle Original Software von Apple welche Sie deinstalliert haben, nun wieder installiert wird (Mail, iPhoto, usw.).

Viele Power User möchten wissen was und wo installiert wurde. Da es nun mit OS X nicht mehr genügt im Systemordner die alten Erweiterungen mit Etiketten zu markieren. Innerhalb eines solchen .pkg files gibt es in den im Ordner Ressourcen ein „.bom" (bill of material) File.

Um dieses File zu lesen gibt es in der Konsole den „lsbom" Befehl. Um den Inhalt des Security Update vom 20.9.2002 einzusehen sieht das dann wie folgt aus:

```
[TitanSurfer:/] pts% sudo lsbom /Library/Receipts/SecurityUpd2002-09-
20.pkg/Contents/Resources/SecurityUpd2002-09-20.bom
Password:
.        41775   0/80
./Applications  40775   0/80
./Applications/Utilities        40775   0/80
./Applications/Utilities/Terminal.app   40775   0/80
./Applications/Utilities/Terminal.app/Contents  40775   0/80
```

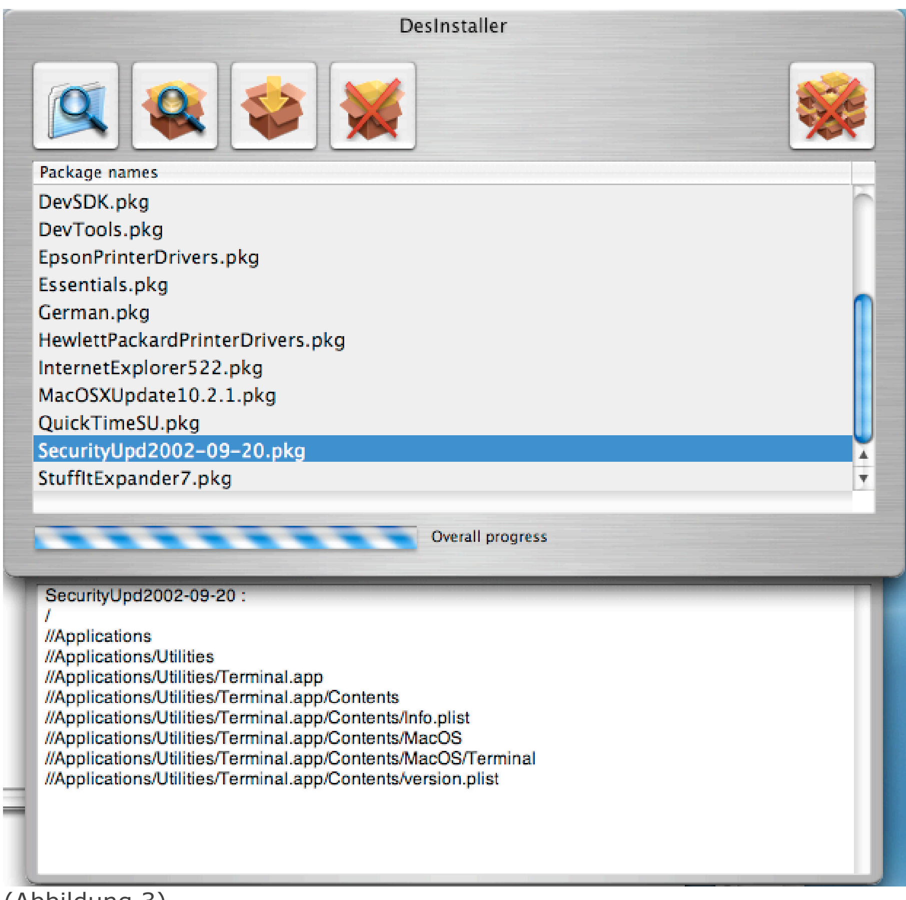
```
./Applications/Utilities/Terminal.app/Contents/Info.plist       100664
0/80    2595    3060271716
./Applications/Utilities/Terminal.app/Contents/MacOS    40775   0/80
./Applications/Utilities/Terminal.app/Contents/MacOS/Terminal   100775
0/80    295136  436161111
./Applications/Utilities/Terminal.app/Contents/version.plist    100664
0/80    471     2295228637
[TitanSurfer:/] pts%
```

Zur Verdeutlichung:

1. Zeile sudo (Der Adminbenutzer machte diesen einen Befehl) lsbom (Der Befehl zur Einsicht von .bom Files) der ganze Pfad zum File.
2. Passwort Eingabe des Adminbenutzers
3. Die Ausgaben mit den Dateien welche ersetzt wurden und die Orte wo sie hinkopiert wurden.

Deinstallieren

.bom File zeigen uns also die Dateien welche installiert wurden. Das Deinstallieren ist jedoch nicht so einfach. Das Problem ist hier offensichtlich. Wenn ich alle Dateien welche ich im Beispiel für lsbom von oben einfach lösche, habe ich zwar das Security Update deinstalliert, habe aber gleichzeitig unter anderem auch das Terminal gelöscht. Das gleiche gilt für Shareware Produkte wie „desinstaller" (Abbildung 3).



(Abbildung 3)

Falls ich also ein kritisches Update einspiele, ist es „zur Zeit“ sinnvoll, dass ich eine Kopie von meinem System ziehe um nötigenfalls mit den Informationen vom .bom File alles wieder deinstallieren kann und durch die alten Dateien ersetzen kann. Mit „zur Zeit“ meine ich, dass es vermutlich bald eine Funktion geben wird, welche uns automatisch eine Kopie erstellt und sie gegebenenfalls automatisch zurückspielen kann. Shareware Programme wie „Desinstaller“ aus Abbildung 3 können diesen Vorgang natürlich auch per Mausklick durchführen. Allerdings haben sie das gleiche Manko wie wenn Sie es manuell durchführen, auch bei Desinstaller wird das Terminal gelöscht. Also seien Sie mit deinstallieren unter OS X sehr vorsichtig und machen Sie lieber einmal mehr Backup.

Bundles

Wie wir im Pfad der eingespielten Files ersehen sind Programme eigentlich keine Programme wie sie im klasischen OS gewesen sind. Unter OS 9 wurden die Dateien, welche das Programm zusätzlich benutzte, in verschiedenen Orten und Formen abgelegt. Zum Beispiel als Shared Library in den Systemerweiterungen. Das Programm selber war in zwei Teile (forks) aufgeteilt. Ein „data fork“ welches den ausführbaren PPC Code enthielt und „resource fork“. Der „resource fork“ enthielt Vorlagen für verschiedene Elemente welche für den Benutzer sichtbar waren. Wie etwa Menueinträge, Dialoge und Fenstertypen. In OS X wurde das geändert. Man spricht jetzt von „bundles“. Ein „bundle“ ist eine Sammlung von Datenelementen (ausführbarer Code und Ressourcen Informationen) . Jeder Typ wird durch ein einzelnes File repräsentiert. Diese Files werden zusammengenommen und bilden dann ein Directory mit der Endung „.app“. Sie präsentieren sich dem Benutzer dann als Programmsymbol welches man zum starten doppelklicken kann. Das wichtigste nochmals: Unter OS X sind Programme „bundels“ und kein einzelnes File mehr. Bundles oder Programme können mit einem CTRL + Mausklick geöffnet werden. Zur allgemeinen Verwirrung werden „bundles“ auch manchmal „packages“ genannt.

Diagnose

Mit einem komplexen Betriebssystem wie OS X kann immer einiges schief gehen. Und wie immer bleibt uns Benutzern ganz wenig übrig um vor unserem PC das Beste aus der Situation zu machen. Doch ganz wehrlos sind wir nicht. Defekte Mac OS X Installation reparieren und defekte Disk korrigieren sind Vorgänge, welche wir mit booten von der Original CD aus erledigen können. Aber was liegt sonst noch drin:

Verbose Boot

Mac OS 8 und 9 hielten die meisten der System Operationen vom Benutzer fern und liessen uns im Glauben, dass unser Betriebssystem nur aus Systemerweiterungen und Kontrollfeldern bestehe. Wenn OS X startet, werden dutzende von Support Prozessen und Treiber zur gleichen Zeit geladen. Wenn etwas falsch geht, ist es der Vorstellung des Benutzers überlassen zu raten was genau falsch gegangen ist. In den meisten Fällen wissen wir Benutzer nicht einmal, dass mit der Systemkonfiguration etwas falsch gelaufen ist. Dies deshalb weil der ganze Boot Vorgang (boot strap) hinter einem sehr simplen GUI Start Screen versteckt ist.

Um genau zu beobachten was während dem Bootvorgang abläuft, drückt man unmittelbar nach dem Drücken des Startknopfs die Tastenkombination Command + V. Dies forciert dann einen „Verbose Boot“. In diesem Modus werden alle Status- und Fehlermeldungen des ganzen Bootvorgangs angezeigt. Statt eines grauen Bildschirms, sehen wir nun Zeile um Zeile Meldungen. O.K. dies sieht ein bisschen wie der Start eines Windowsrechner aus, dafür fühlen sich nun Windows und Linux Benutzer wie zuhause.

Wenn der Computer also während des Bootvorganges irgendwo hängen bleibt lohnt es sich schnell im Verbose Mode zu booten, um exakt zu analysieren bei welchem Vorgang er hängen bleibt.

Startprobleme, blauer Bildschirm
Die wenigsten der Benutzer können nun aber aus den Informationen des Verbose Boot irgend eine Information herausziehen welche sie weiter bringt. Schauen wir uns einmal an welches die häufigsten Startprobleme sind.

Situation: Der Bildschirm ist blau und der farbig drehende Cursor ist zu sehen und dreht und dreht und dreht....

1. Mac OS X schaut im Zeichensatz Ordner von OS 9 nach ob er Schriften laden kann. Eine defekte Schrift kann also diesen Fehler verursachen. Um das zu beheben startet man von der OS 9 CD und zieht den ganzen Zeichensatz Ordner von OS 9 auf das root Level von OS X, oder sonstwohin wo man ihn wiederfindet. Neustart und beten dass es nun geht.

2. Brachte das nichts, probiert man es mit den Startup Items. Diese werden erst geladen wenn das System schon fast initialisiert ist. Sie sind mit den Startobjekten von OS 9 nur bedingt vergleichbar. Dazu startet man wieder ab der OS 9 CD und entfernt temporär alle Startup Items aus den folgenden Ordnern: /Library/StartupItems und /System/Library/StartupItems.

3. Modem Benutzer können ein Problem haben, weil sie in der Netzwerkeinstellung bei den PPP Optionen „automatisch Verbinden" angeklickt haben und OS X beim Anmelden das Modem initialisiert und das System sich probiert irgendwo im Internet zu verbinden. Hierzu muss man die Netzwerkeinstellungen ganz zurücksetzen. Das heisst die Preferenz Datei löschen. Um das zu tun ohne das man OS X starten kann, muss man im „single user mode" booten.

Der Single User Mode
Um in den Single User Modus zu kommen muss man beim Start die Command + S Kombination gedrückt halten. Der „single user mode" erlaubt es einem Administrator direkt, durch ein Command Line Interface auf das System zuzugreifen.

Das ist die letzte und entscheidende Methode wenn ein System nicht mehr startet und sollte nur gebraucht werden wenn gar nichts mehr geht. Der Single User Mode betätigt Befehle mit vollen „root" Rechten. **Der Single User Mode ist ein schlechter Ort um sich ein bisschen auf der Platte umzuschauen oder Unix zu lernen.**

Der Single User Mode startet in einem „text only" Modus wie der Verbose Mode. Der Prozess endet indem er den Benutzer in einer Shell empfängt.

```
Singleuser boot – fsck not done
Root device is mounted read-only
If you want to make modifications to files,
run '/sbin/fsck –y' first an them 'sbin/mount –uw /'
localhost#
```

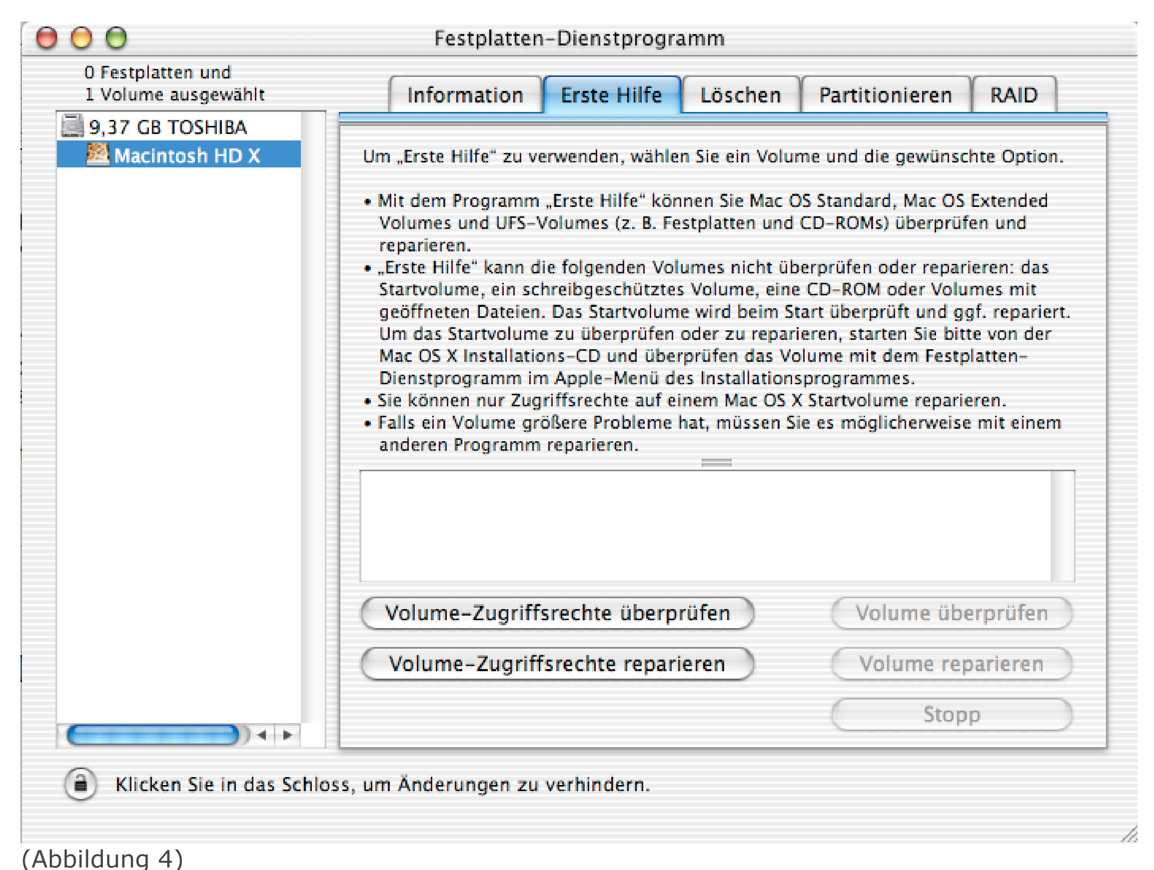
Um jetzt nun die Preferenz Datei zu löschen geht man wie folgt vor:

1. Wie es in der Shell steht, wollen wir Modifikationen vornehmen. Also tippen wir **mount –uw/**
2. Danach Return zum bestätigen des Befehls.
3. **mv /var/db/SystemConfiguration/preferences.xml preferences.old**
4. Den Befehl wieder mit Return bestätigen. Hiermit wird die Original Datei gelöscht und in einen neuen Namen umbenannt (preferences.old).
5. **reboot**
6. Danach Return zum Bestätigen des Befehls und zum Neustarten des Rechners.

Achtung: Alle Einstellungen in den Netzwerkeinstellungen müssen neu gemacht werden, wenn Sie die Datei „preferences.xls"gelöscht haben. Falls das Löschen der Preference Datei nicht das gewünschte Resultat brachte, können Sie nun immer noch die Datei „preferences.old" wieder in „ preferences.xml" umbenenen.

Hat man irgendwas an der NetInfo Datenbank geändert bringt es eventuell etwas wenn man die Suchpfade löscht. Dies geschieht mit:
rm /Library/Preferences/DirectoryService/SearchNodeConfig.plist.

Wenn der Rechner nach vielem Konfigurieren nicht mehr hochkommt kann es sein, dass mit den Berechtigungen etwas nicht stimmt und dass dem System nicht mehr genügend Rechte zugesprochen sind um etwas zu lesen oder auszuführen.
Wenn das System normal läuft kann man diesem Problem mit dem Dienstprogramm „Festplatten-Dienstprogramm" im Reiter „Erste Hilfe" beheben (Abbildung 4). Allerdings sind wir hier in der Situation, dass unser System nicht mehr läuft und wir diese Korrekturen per Konsole ausführen müssen.



(Abbildung 4)

Um die Berechtigungen im Single User Mode zu korrigieren gehen wir wie folgt vor:

1. Wieder im Single User Mode starten
2. **fsck –y**
3. Mit Return bestätigen um das FileSystem (fsck) zu prüfen und alle Fragen ob man diesen Block reparieren soll oder nicht mit Ja beantworten (-y).
4. **mount –uw**
5. Return mountet die Platte mit Schreibberechtigung.
6. **chmod 1775 /**
7. Return ändernt den Zugriffs Modus für alle Dateien auf der Platte-
8. **reboot**
9. Return startet den Rechner neu.

Hinweis:
Der Befehl „**SystemStarter –g**" startet OS X inkl Aqua vom „single user mode" aus.
Der Befehl „**fsck**" (file system check) ist equivalent zum „Erste Hilfe" Programm.
Der „**man**" Befehl funktioniert auch im „single user mode".
Weitere wichtige Konfigurationsfile finden sich auch unter:

/etc/hostconfig

/privat/var/db/SystemConfiguration/preferences.xml

Diese Files beinhalten die Netzwerk- und Bootinformationen des Rechners.

Im „single user mode" sind noch keine Tastaturlayouts geladen. Siehe dazu Seite 20.

Grauer Bildschirm während dem Starten
Ein grauer Bildschirm während dem Starten zeigt an, dass ein Fehler augetaucht ist der eher weniger mit Software, sondern mit Hardware zu tun hat. Denn hier wird ganz offensichtlich das System nicht gestartet. Doch was ist zu tun?

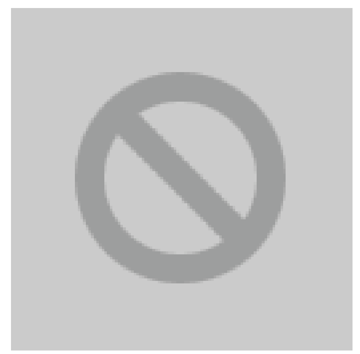
1. Alle externen Peripherie wie FireWire, USB, PCMCIA-Gerät ausstecken. Wenn der Rechner nach Neustart startet, ein Gerät nach dem anderen wieder einstecken bis man den Übeltäter gefunden hat. Hat man das Gerät gefunden. Sollte man auf zwei Dinge achten:
    a. Habe ich die aktuellen Geräte Treiber für das Produkt?
    b. Habe ich für alle anderen Geräte welche ich noch betreibe, aktuelle Treiber? Denn es könnte gut sein dass ein anderer Treiber das Problem in Zusammenarbeit mit anderen Treibern verursacht.
    c. Habe ich die aktuelle Firmware für meinen Mac?

2. Hat das nichts gebracht, vergessen Sie nicht die SCSI Karten aus dem PCI Slot zu entfernen.

3. Sie haben keine SCSI Karte! Enfernen Sie die RAM Bausteine einzeln und probieren Sie so zu starten.

4. Hat auch nichts gebracht! Probieren Sie noch einmal kurz ab der Original CD zu Booten und Erste Hilfe auf der Systemplatte ausführen. Nichts gebracht. Tja, nun ist guter Rat teuer. Begeben Sie sich in die Support Hölle von Apple Computer. Viel Glück und gute Nerven wünsche ich Ihnen.

„Verbot Zeichen" oder einen „zerbrochenen Ordner" beim booten
Eine „Verbot" Zeichen (OS X 10.2) (Abbildung 5), oder einen „zerbrochenen Ordner" (OS X 10.1) während dem Starten signalisiert das etwas mit den Systemdateien nicht in Ordnung ist.


(Abbildung 5)

Einige der für Mac OS X wichtigen Files sind unsichtbar wenn man Mac OS X startet. Wie etwa der „mach_kernel". Sie werden sichtbar, wenn man unter OS 9 startet oder Software gebraucht, welche unsichtbare Files anzeigen können. Es ist wichtig, diese Files weder zu löschen, zu verschieben, umzubenennen, oder ihre Zugriffs-berechtigung zu verändern. Macht man das trotzdem kann das dazu führen, dass OS X nicht mehr starten kann. Hier eine Liste der Files welche auf dem root Level der Festplatte sind und dort gelassen werden müssen:

mach_kernel (unsichbares File)
Application (sichtbarer Ordner)
automount (unsichtbarer Ordner)
Library (sichtbarer Ordner)
System (sichtbarer Ordner)
Users (sichtbarer Ordner)

Wenn aber alle Dateien unverändert sind, und Sie hoch und heilig schwören nichts angefasst zu haben?

1. Dann gilt es wie früher zuerst das Parameter RAM/NVRAM zu löschen. Wie Sie das genau für Ihren Rechnertyp durchführen finden im „technical document 2238" auf www.info.apple.com.

2. Starten Sie dann erneut und drücken Sie die Taste „X" während Sie starten. Das zwingt den Rechner ab OS X zu starten.

3. Wenn das auch nicht klappt, starten Sie ab der OS 9 CD und öffnen Sie das Kontrollfeld „Startvolumen". Wählen Sie den OS X Ordner aus und starten Sie den Rechner neu.

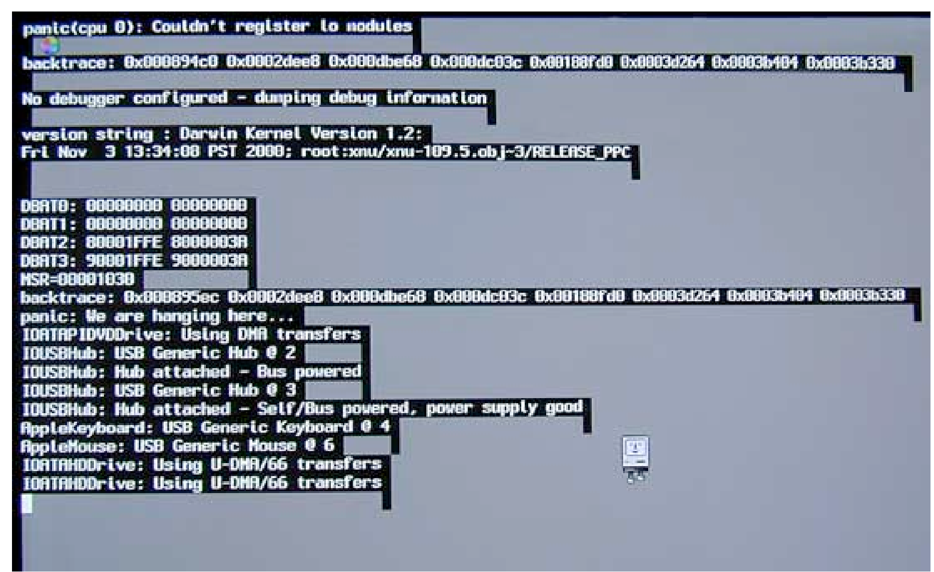
4. Klappt das auch nicht, werden Sie nervös und schnappen sich die Original OS X mit der Version welche Sie installiert haben. Starten Sie dann wieder ab OS 9. Wenn der Mac gestartet ist, legen Sie die OS X CD ein. Kopieren Sie jetzt vom root der OS X CD den „mach_kernel". Ersetzen Sie ihn auf dem OS X Startvolumen. Markieren Sie nun im Startvolumen Kontrollfeld wieder OS X. Starten Sie den Rechner neu.

5. Beachten Sie, dass die Dateien „mach" und „mach.sym", falls sie irgendwie fehlen, automatisch generiert werden.

6. Falls das auch nicht zum Erfolg geführt hat, müssen Sie das System aktualisieren.

Kernel panic
Der „kernel panic" ist ein Fehler welcher auftritt, wenn der Kern (kernel) des Betriebssystems eine Instruktion in einem unerwarteten Format bekommt, oder er eine Instruktion nicht sauber bearbeiten kann. Ein „kernel panic" kann aber auch eintreffen wenn das Betriebssystem einen aufgetretenen Fehler nicht sauber auffangen kann. Vielfach ist Software an einem „kernel panic" schuld. In einigen Fällen aber auch defekte oder inkompatible Hardware.

Ein „kernel panic" manifestiert sich zwischen OS X 10.1 und 10.2 unterschiedlich. Unter 10.1 erscheint weisser Text auf schwarzem Hintergrund (Abbildung 6).



(Abbildung 6)

Mit Mac OS X 10.2 wurde ein automatisches „kernel panic logging" eingeführt. Dieses Logfile gibt den Fehlermeldungstext des Kernels wieder, solange man das PRAM nicht gelöscht hat. Da der Rechner bei einem „kernel panic" zwingend neu gestartet werden muss. Der „kernel panic" Text wird dem Logfile angehängt wenn das OS das nächste mal hochfährt. Der Dateiname ist panic.log und wird auf der Startdisk unter:

/Library/Logs/

gespeichert.

Ein „kernel panic" wird unter OS X 10.2 ebenfalls visuell angezeigt. Eine Meldung „You need to restart your computer" (Abbildung 7) erscheint.

You need to restart your computer. Hold down the Power button for several seconds or press the Restart button.

Veuillez redémarrer votre ordinateur. Maintenez la touche de démarrage enfoncée pendant plusieurs secondes ou bien appuyez sur le bouton de réinitialisation.

Sie müssen Ihren Computer neu starten. Halten Sie dazu die Einschalttaste einige Sekunden gedrückt oder drücken Sie die Neustart-Taste.

コンピュータを再起動する必要があります。パワーボタンを数秒間押し続けるか、リセットボタンを押してください。

(Abbildung 7)

Das „kernel panic" Logfile enthält Informationen welche Entwicklern helfen die Software besser zu entwicklen. Das Logfile gibt Auskunft über den Status des Rechners zur Zeit des Absturzes.

Bei einem Systemstart welcher in einem „kernel panic" endet haben wir gesehen, dass Treiber und Hardware schuld sein können. Ebenfalls das verschieben oder umbenenen oder modifizieren von systemrelevanten Dateien auf dem root. Siehe Abschnitt „verbot Zeichen".

Bei Hardware bedingten Fehlern wird oftmals ein „Firmware Update" zum Beheben des Fehlers angeboten. In den meisten Fällen muss man dann schnell im OS 9 booten um die Firmware auf die Hardware zu spielen. So ist zur Zeit (bis 1.1.2003) die OS 9 CD unser Freund und Helfer beim Beheben von OS 10 Problemen.

Maintenance

Der Unterhalt einer OS X Installation ist ein Thema bei welchem sich die Meinungen zu teilen beginnen. Ich möchte mich hier nicht auf die endgültige, allumfassende Methode festlegen, sondern aufzeigen was ich anwende.

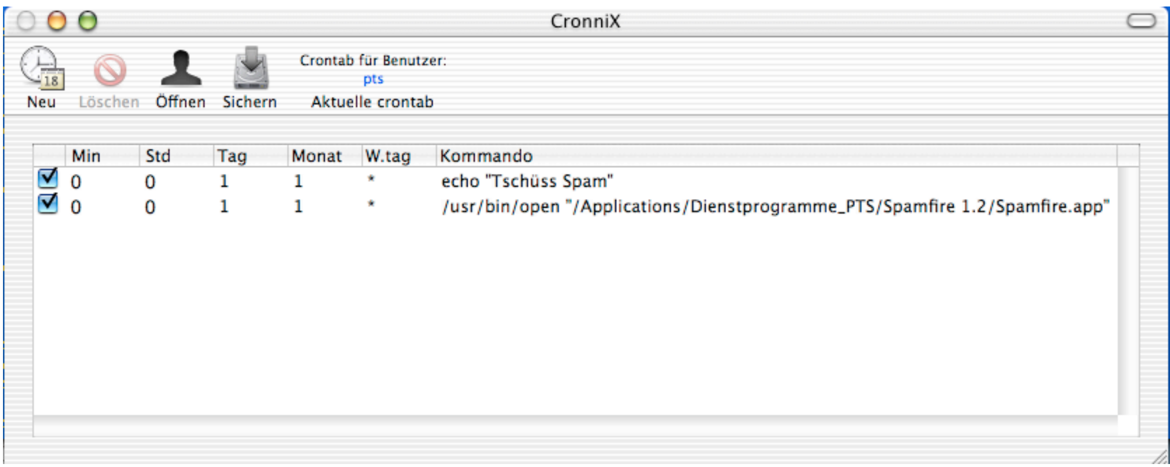
Der cron Befehl

Cron wird benutzt um Befehle zeitgesteuert auszuführen. Auf Systemebene wird die Datei /etc/crontab ausgelesen. Dort sieht man, dass drei verschiedene Scripts ausgeführt werden nämlich:

/etc/daily	Entfernt den täglich scratch und junkfile Müll.
/etc/weekly	Remove den wöchentlichen scratch und junkfiles Müll, lookupd.log, lpr.log, mail.log, netinfo.log und ftp.log.
/etc/monthly	Entfernt den monatlichen scratch und junkfile Müll.

Diese Scripts werden automatisch ausgeführt. Natürlich kann ich meine schnelle Reinemache von Hand ausführen via **sudo sh /etc/weekly**. Hier hat aber Sven Schmidt ein cooles Tool geschrieben welches die Cron Scripts wunderbar verwaltet und auch per Mausclick ausführen lässt (Abbildung 8).

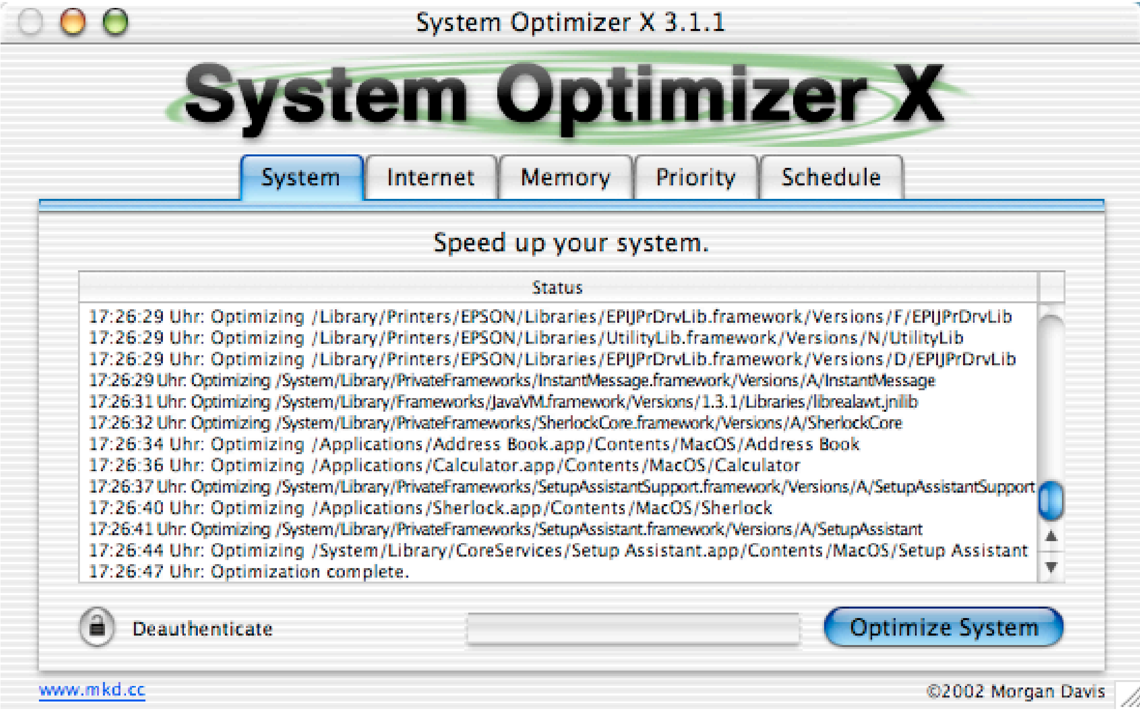
CronniX



(Abbildung 8)

Zu finden ist dieses Tool unter www.koch-schmidt.de.

System Optimizer X
Ebenfalls ein lästiges Ding sind die prebindings, sowie die Systemoptimierung welche ihnen zugesprochen wird. Auch hier können wir die .pkg's schnell mit dem Terminbefehl **sudo update_prebinding -root / -force** „manuell" updaten. Wir können es aber einem kleveren Tool überlassen, dem SOX (Abbildung 9).



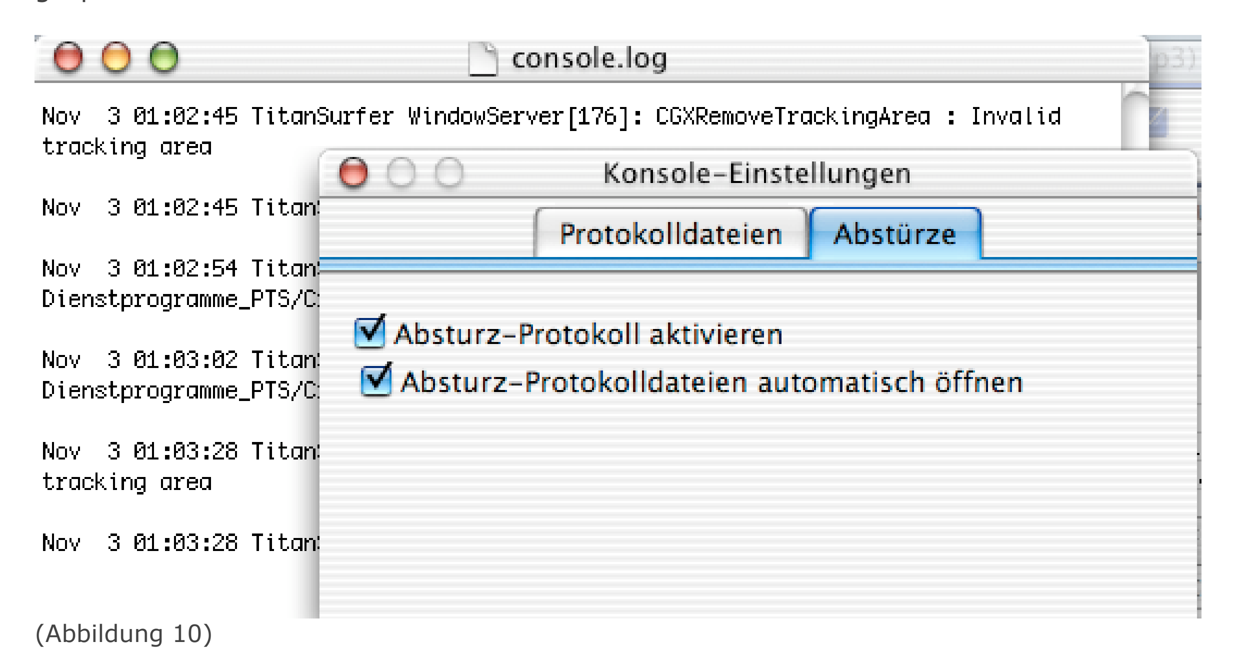
(Abbildung 9)

SOX hat noch einiges in Sachen Optimierung auf Lager. Einfach mal rein schauen und ein „Schedule" setzen (klar ein cron). Download unter www.mkd.cc.

Die Konsole
Nicht vergessen im Dienstprogramm „Konsole" (Abbildung 10) das Crashloging einzuschalten. So sieht man immer welches Programm wann und warum abgestürzt ist. Die Logfiles werden unter

/Users/eigenerBenutzer/Librarys/Logs/CrashReporter

gespeichert.



(Abbildung 10)

Logfiles suchen mit locate und grep
Nicht jede Software speichert ihr Logfiles im selben Ort. Entweder man weiss von jeder Software wo es seine Logfiles ablegt, oder man sucht sie schnell. Der „locate" ist für mich einer der wichtigen Befehle für das Suchen von Dateien im Terminal. Um hier ein schnelles Resultat zu haben, update ich von Zeit zu Zeit meine Datenbank mit dem Befehl:

sudo /usr/libexec/locate.updatedb

Dies ist vergleichbar mit dem Index von Sherlock. Nur geht es 2 Minuten und nicht 48 Stunden. Danach kann man mit dem Befehl **locate** in dieser Datenbank suchen. Um die Suche zu verfeinern kann man die Ausgabe von locate mit grep filtern. (Mehr zu grep und locate im 3. Teil.)

```
[TitanSurfer:~] pts% locate ftp | grep log
/private/var/log/ftp.log
[TitanSurfer:~] pts%
```

1. Zeile: ich suche mit locate nach Files und Ordner welche „ftp" in ihrem Namen haben. Wenn ein Name zutrifft, wird noch mit grep untersucht ob „log" irgendwo im Namen steht.

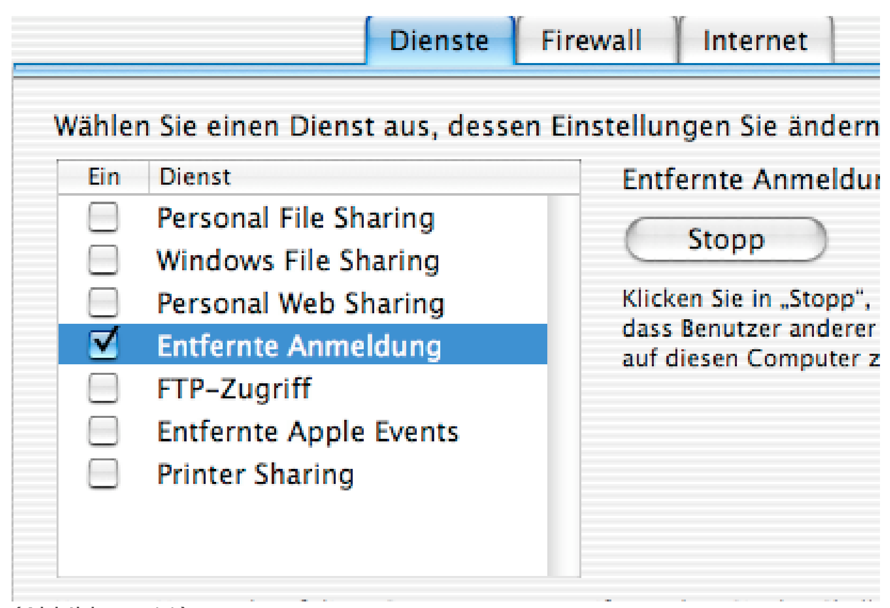
2. Zeile: Ausgabe des Files und des Pfades dazu.

Logfiles überwachen mit ssh und tail
Der Befehl tail ist ein Werkzeug um Files in einem Terminal zu beobachten. Mit diesem Tool kann ich mir permanent anzeigen lassen was gerade dem File angehängt wurde. Dies eignet sich sehr gut um Logfiles zu beobachten. Der Syntax ist einfach

tail –f ftp.log

Die Option –f bewirkt, dass die neuen Eingaben im Zielfile sofort in der Shell wiedergegeben werden.

Um einen FTP Server zu beobachten welcher zum Beispiel im Büro neben an steht. Kann man sich mit ssh am anderen Rechner anmelden. Um SSH Zugriff zu kriegen muss man im Kontrollfeld Sharing die Checkbox „Entfernte Anmeldung" aktiviert haben (Abbildung 11).



(Abbildung 11)

Danach können Sie sich einen Benutzer einrichten, oder mit dem selben Benutzer der schon auf dem Rechner Administrationsrechte hat. Falls Sie nur ein Benutzer haben, melden Sie sich mit diesem an und wechseln zum root Benutzer wenn Sie angemeldet sind.
Im Beispiel melden wir uns als Benutzer pts an den Rechner 10.0.0.19, um uns das ftp.log aktualisiert mit tail anzeigen zu lassen.

Die Beschreibung habe ich in diesem Beispiel direkt in den Terminal Output geschrieben. Fett sind dabei die besprochenen Befehle. Fett und „kursiv" sind meine Kommentare dazu. Beachten Sie auch das Prompt, welches beim „root" Benutzer zu einem # wechselt.

```
Last login: Thu Nov  7 15:51:55 on ttyp5
Welcome to Darwin!
[TitanSurfer:~] pts% ssh pts@10.0.0.19 (Anmelden, vom TitanSurfer aus)
pts@10.0.0.19's password: (Passwort vom Benutzer pts auf 10.0.0.19)
Last login: Thu Nov  7 16:12:14 2002 from 10.0.0.15 (Angemeldet)
Welcome to Darwin!
```

```
[SilverSurfer:~] pts% su root  (In die root Shell wechseln, Rechner ist
Password:                      jetzt Silversurfer)
[SilverSurfer:/Users/pts] pts# locate ftp | grep log (FTP File suchen)
/private/var/log/ftp.log
/private/var/log/ftp.log.0.gz (Die Ausgabe von locate und grep)
[SilverSurfer:/Users/pts] pts# tail -f/private/var/log/ftp.log

(tail gibt das File in das Terminal aus)
Oct 25 01:12:21 SilverSurfer ftpd[462]: FTP LOGIN FROM 10.0.0.14 as pts
(class: real, type: REAL)
Oct 25 01:19:21 SilverSurfer ftpd[588]: connection from 10.0.0.14 to
10.0.0.19
Oct 25 01:19:21 SilverSurfer ftpd[588]: FTP LOGIN FROM 10.0.0.14 as pts
(class: real, type: REAL)
Oct 25 01:20:26 SilverSurfer ftpd[594]: connection from 10.0.0.14 to
10.0.0.19
Oct 25 01:20:26 SilverSurfer ftpd[594]: ANONYMOUS FTP LOGIN REFUSED FROM
10.0.0.14
Oct 25 01:20:52 SilverSurfer ftpd[595]: connection from 10.0.0.14 to
10.0.0.19
Oct 25 01:20:52 SilverSurfer ftpd[595]: ANONYMOUS FTP LOGIN REFUSED FROM
10.0.0.14
Oct 25 01:20:59 SilverSurfer ftpd[595]: FTP LOGIN FROM 10.0.0.14 as
laptop (class: real, type: REAL)
Oct 25 01:30:32 SilverSurfer ftpd[653]: connection from 10.0.0.14 to
10.0.0.19
Oct 25 01:30:32 SilverSurfer ftpd[653]: FTP LOGIN FROM 10.0.0.14 as
laptop (class: real, type: REAL)
^C (ctrl + x um den tail Prozess zu unterbrechen)
[SilverSurfer:/Users/pts] pts# exit (Exit um die root Shell zu beenden)
exit
[SilverSurfer:~] pts% logout (Vom SilverSurfer abmelden)
Connection to 10.0.0.19 closed.
[TitanSurfer:~] pts% (Bin wieder auf meinem Rechner TitanSurfer)
```

Timestamp

Wenn man sich Konfigurationsfiles für seine Applikationen sucht, kann man zwischendurch schon mal verzweifeln. Kreuz und Quer über die Boot Harddisk sind sie verteilt. UNIX bietet hier eine Hilfe an mit der man sich ein bisschen schlauer machen kann. Mit Timestamps ist es möglich alle Files welche seit dem erstellen des Timestamps geändert wurden aufzuzeichnen. So können Sie nun Änderungen an den Einstellung vornehmen und nachher schauen was und wo geändert wurde. Gehen Sie dazu wie folgt vor:

```
[TitanSurfer:~] pts% sudo –s (Root aktivieren)
Password:
[TitanSurfer:~] root# touch ~/timestamp (Den Timestamp aktivieren)
Jetzt die Änderuneg an dem Programm vornehmen welches Sie beobachten
wollen. Falls das passiert ist gehen Sie zum nächsten Befehl.
[TitanSurfer:~] root# find -x / -newer ~/timestamp >~/aenderungen.txt
Mit diesem Befehl lesen Sie die Timestamp aus und schreiben Sie die
Änderungen in eine Textdatei. Diese wir in Ihrem Home Verzeichnis
gespeichert.
[TitanSurfer:~] root# exit
```

Ich habe für dieses Beispiel bei mir Transparenz des Terminalfensters verändert. Das Logfile sieht dann wie folgt aus:

```
/automount
/Network/Servers
/private/var/log/system.log
/private/var/tmp/console.log
/Users/pts
/Users/pts/aenderungen.txt
/Users/pts/Library/Preferences
/Users/pts/Library/Preferences/com.apple.Terminal.plist
```

Somit ist klar dass die Einstellungen in com.apple.Terminal.plist File gespeichert sind.

Prozessmanagment
Unter OS X werden alle Programme in einem Prozess ausgeführt. Jedes Programm oder jeder Deamon welcher das System startet, wird als ein eigener Prozess welcher eine eigene PID (Process ID) erhält, verarbeitet. Mit dem Befehl **ps –aux** (zu den Optionen aux bitte die man page lesen). Kann ich mir alle Prozesse welche auf meinem System laufen anzeigen lassen. Ebenfalls ersichtlich ist dort die PID Nummer.

```
[TitanSurfer:~] pts% ps -aux
USER   PID %CPU %MEM      VSZ    RSS  TT  STAT STARTED      TIME COMMAND
pts    1483    9.4   6.8     94136   26552   ??   S       1:17PM    0:42.39
/Applications/Microsoft Office X/Microsoft Word
```

So ist ersichtlich, dass MS Office in dem ich arbeite die PID 1483 hat. Angenommen ich habe ein Programm (Prozess) welches sich nicht mehr schliessen lässt und ich mit „force quit“ nicht weiterkomme. So zeige ich mir mit ps –aux die Prozessliste an. Um herauszufinden welche PID meine Problemsoftware besitzt.

Wenn man weiss wie der Prozess heisst und man viele Prozesse am Laufen hat, und hier nicht die Liste durchsuchen möchte, kann man das Ganze natürlich auch mit grep filtern. Wenn ich nun nach meinem „Word“ suche, sieht es dann so aus:

```
[TitanSurfer:~] pts% ps -aux | grep Word
pts   1483  21.5  8.3    99456  32584  ??  S     1:17PM   4:35.18
/Applications/Microsoft Office X/Microsoft Word /Applications/Microsoft
Office X/Mic
pts   1526   0.0  0.0     1116      4 std  R+    1:39PM   0:00.00 grep
Word
```

Zweite bis vierte Zeile sind der Output (nicht ganz alles). Die fünfte Zeile ist ein weiterer Prozess welche grep auch herausfiltert, da er ebenfalls das Wort „Word“ enthält. Nämlich, sich selber. Also, der Prozess grep.

Grep kann mit der Option –v auch Ausschlüsse vornehmen. Wenn man also den grep Prozess nicht ausgegeben haben möchte, müsste der Befehl so aussehen:

ps -aux | grep Word | grep -v grep

Das aber nur so am Rande.

Angenommen mein „Word“ hat sich irgendwie aufgehängt. Ist ja nicht ganz aus der Luft gegriffen. Wie auch immer. Ich habe hier die PID 1483 und kann nun mit dem Befehl **kill** diesen Prozess beenden, oder eben killen.

kill 1483

Wenn dieser Prozess vom System gestartet wurde, muss ich mich eventuell zuerst als root ausgeben um ihn zu stoppen. Aber „Word" habe ich als User gestartet. So ist es mir erlaubt, dass Ganze auch wieder zu beenden.

Was aber wenn kill, den Prozess nicht beendet? Wenn kill nicht zum Erfolg führt, hat dieser Befehl eine ganze Reihe von Optionen. Die „tödlichste" ist die Option **–9**.

```
kill –9 1483
```

Die –9 Option steht für „non-ignoreable kill". Wenn dieser Befehl nicht geht, dann geht gar nichts mehr. Und Sie müssen Ihrem Rechner vermutlich den Strom wegnehmen um ihn neu zu starten, da OS X den Prozess beim herunterfahren, ebenfalls nicht stoppen kann und so stehen bleibt.

Solche Stopp Massnahmen gefährden natürlich die Integrität des File Systems. An OS X 10.2.2 hat Apple hier eine Möglichkeit eingebaut das Ganze noch stabiler zu machen als es bisher mit HFS schon war.

Das File System Journaling

Hier wird das HFS+ File System mit einem Journalfile ausgestattet in welchen die vitalen Vorgänge innerhalb des Dateisystems gelogt werden, so dass der Status des File Systems aus einer Datei ersichtlich ist und nicht wieder hergestellt werden muss. Dies rettet Ihnen im Falle eines Absturzes zwar keine Daten welche Sie gerade, zum Zeitpunkt des Absturzes, am speichern gewesen sind, jedoch ist die Struktur der Festplatte gewährleistet. Dies hilft vor allem beim Neustart eines abgestürzten Rechners. Da das überprüfen und wiederherstellen einer defekten Partition schon mal ein paar Stunden in Anspruch nehmen kann. Vor allem bei grösseren Festplatten und Servern.

Ganz allgemein kostet Sie das Erstellen des Journals einen gewissen Prozentsatz an Leistung. Man spricht von 10%. Wobei diese Zahl zur Zeit noch nicht signifikant ist.

Wie schalte ich das Journaling HFS+ nun ein? Gehen Sie dazu in die Konsole und gehen Sie wie folgt vor. Überprüfen Sie zuerst die HFS Struktur Ihrer Festplatte. Um herauszufinden welche Partition Ihrer Festplatte mit HFS formatiert ist, zeigen Sie sich die Partitionsliste mit folgendem Befehl an:

```
[TitanSurfer:~] pts% sudo diskutil list
/dev/disk0
   #:                   type name               size      identifier
   0: Apple_partition_scheme                    *9.4 GB   disk0
   1:    Apple_partition_map                    31.5 KB   disk0s1
   2:         Apple_Driver43                    28.0 KB   disk0s2
   3:         Apple_Driver43                    28.0 KB   disk0s3
   4:       Apple_Driver_ATA                    28.0 KB   disk0s4
   5:       Apple_Driver_ATA                    28.0 KB   disk0s5
   6:         Apple_FWDriver                    256.0 KB  disk0s6
   7:     Apple_Driver_IOKit                    256.0 KB  disk0s7
   8:          Apple_Patches                    256.0 KB  disk0s8
   9:              Apple_HFS Macintosh HD X     9.4 GB    disk0s9
```

So ist ersichtlich, dass die Partition 9 mit dem Identifier „disk9s9" in Apple_HFS initialisiert ist. Nun können Sie diese Partition überprüfen:

```
[TitanSurfer:~] pts% sudo fsck_hfs /dev/disk0s9
** /dev/rdisk0s9
```

```
** Root file system
** Checking HFS Plus volume.
** Checking Extents Overflow file.
** Checking Catalog file.
.......
.......
```

Wenn hier alles o.k. ist kann man nun auf seinem FileSystem das Journaling starten. Dies geschieht mit folgendem Befehl:

sudo diskutil enableJournal / (Für die Systemdisk)

sudo diskutil enableJournal /Volumes/2Platte (Für eine Festplatte namens „2 Platte“)

Das Entfernen der „journaling Funktion“ funktioniert ähnlich. Mit dem logischen Befehl:

sudo diskutil disableJournal / (Für die Systemdisk)

sudo diskutil disableJournal /Volumes/2Platte (Für eine Festplatte namens „2 Platte“)

fsck Fehler bei eingeschaltetem JFS
Zu Erwähnen ist noch dass bei eingeschaltetem „Journal“ der Befehl fsck und fsck_HFS Fehler anzeigen welche ignoriert werden können. Dies sind die Fehler:

- Volume bitmap needs minor repair
- Invalid volume free block count
- Volume header needs minor repair
- Incorrect block count for file

Wenn Sie nun fsck brauchen ist es nun zur Sicherheit wichtig das Sie es mit den Optionen –n und –f brauchen, so dass nicht ausversehen das File System modifiziert wird. –n gibt bei allen Fragen zur Reparaturen dem Befehl fsck automatisch ein „Nein“ zurück, während –f den Befehl fsck zwingt den Test weiter zu führen (force).

Das perfekte Pflegen eines Unix Systems füllt Bücher. Ich glaube mit diesen Tools und Inputs hat man einen Grundstock. Nicht zu vergessen das Festplatten Dienstprogramm oder eben den **fsck** Befehl.

Christoph Müller
Rüschlikon, 19.1.2003

Bei Fragen oder Anmerkungen, kontaktieren Sie mich bitte unter chm@pts.ch.

Dank
Mein Dank geht an:

Bettina Kneubühler, für die Zeit welche Sie mir mit meinen Computern lässt.
Erna Wehrlé, für das grammatische Korrekturlesen.
Dave Uhlmann, für das inhaltliche Testlesen.
Thomas Paszti von Mediaforum, für den Webspace und das Promoten der „Consoliero“ Serie.



macosxalliance

Anhang 1: US Tastatur Layout





